(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **05327693 A**

(43) Date of publication of application: **10.12.93**

(51) Int. Cl **H04L 9/06**
H04L 9/14
H04B 7/26

(21) Application number: **02402926**

(22) Date of filing: **17.12.90**

(71) Applicant: **NIPPON TELEGR & TELEPH CORP <NTT> N T T IDOU TSUUSHINMOU KK**

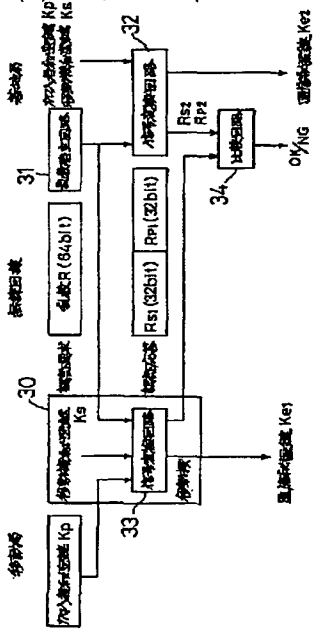
(72) Inventor: **KAMIBAYASHI SHINJI**
KOBAYASHI KATSUMI
ONOE SEIZO
HANAOKA MITSUAKI
NAKAMURA HIROSHI

(54) **AUTHENTICATION METHOD IN DIGITAL MOBILE COMMUNICATION**

(57) Abstract:

PURPOSE: To enable a mobile station to be shared and to prevent illegal use by specifying a authentication confirmation signal and a authentication reply signal of a mobile set and a subscriber with a random number and a secret key and starting the operation when both the signals are coincident.

CONSTITUTION: A random number generating circuit 31 generates at first a random number R for an authentication request in a base station and transmits the number to a mobile station. A mobile set 30 enters the random number R and secret keys K_s, K_p of the mobile set and subscriber to a signal conversion circuit 33 to obtain an authentication reply and a communication ciphering key K_{e1} and transmits the authentication reply to the base station. The base station inputs the random number R and secret keys Ks, Kp to a signal conversion circuit 32 to obtain an authentication reply and a communication ciphering key K_{e2}. A comparator circuit 34 compares a bit pattern of the authentication reply received from the mobile station with a bit pattern of the authentication reply generated in the base station, and enables the authentication of the mobile set when they are coincident and disables the recognition in other cases. That is, then the authentication of the mobile set and the subscriber authentication are implemented simultaneously by one authentication procedure to share the mobile station by plural subscribers without degradation in the throughput.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－327693

(43)公開日　平成５年(1993)12月10日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｈ０４Ｂ	7/26	１０９　Ｓ	7304－5K			
			7117－5K	Ｈ０４Ｌ　9/ 02	Ｚ	

審査請求　未請求　請求項の数２(全　８　頁)

(21)出願番号　特願平2－402926

(22)出願日　平成２年(1990)12月17日

特許法第30条第１項適用申請有り　1990年９月15日　社団法人電子情報通信学会発行の「1990年電子情報通信学会秋季全国大会講演論文集」に発表

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号
(74)上記１名の代理人　弁理士　伊東　忠彦
(71)出願人　392026693
エヌ・ティ・ティ移動通信網株式会社
東京都港区虎ノ門二丁目10番１号
(72)発明者　上林　真司
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内
(72)発明者　小林　勝美
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

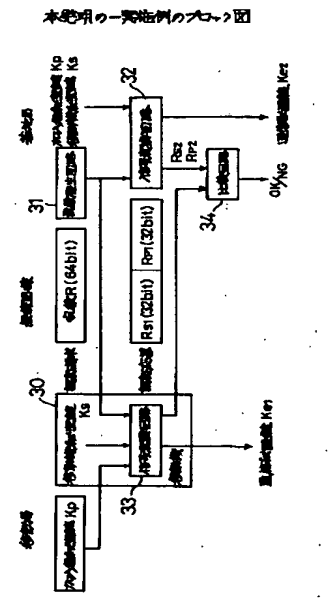
最終頁に続く

(54)【発明の名称】　ディジタル移動通信における認証方法

(57)【要約】

【目的】　本発明はディジタル移動通信における基地局が、通信の相手の移動局が正当な移動局であることを認証するディジタル移動通信における認証方法に関し、無線のスループットの低下を防止して１台の移動機を複数の加入者で共用することができると共に、盗難による不当な使用を防止することを目的とする。

【構成】　移動局において、基地局から送られた乱数Ｒと移動機秘密鍵Ｋs 及び加入者秘密鍵Ｋp より認証応答信号Ｒs1，Ｒp1を生成して基地局に送ると共に秘匿鍵ｋe1を生成する。一方、基地局においても同様にして認証確認信号Ｒs2，Ｒp2を生成して、認証応答信号Ｒs1，Ｒp1と比較し、一致すれば通信を開始するように構成する。また、基地局においても同様にして秘匿鍵Ｋe2を生成する。さらに、秘匿鍵の一部を暗証番号と置換える。



1

【特許請求の範囲】

【請求項１】　移動局側の移動機と基地局との間で移動通信を行うにあたり、通信相手の認証を行い、通信を開始するか否かの判断を行うためのディジタル移動通信における認証方法において、

前記移動局は、

前記基地局より送られた所定の乱数と、予め保持されている移動機固有の第１の秘密鍵とにより第１の特定法則に従って移動機認証応答信号を作成して該基地局に送信し、

該乱数と加入者からの加入者固有の第２の秘密鍵とにより第２の特定法則に従って加入者認証応答信号を作成して該基地局に送信し、

該乱数と該第１及び第２の秘密鍵とにより第３の特定法則に従って通信を秘匿する通信秘匿鍵を作成し、

前記基地局は、

該基地局で発生させた該所定の乱数と、予め保持されている前記第１及び第２の秘密鍵とにより、前記第１，第２及び第３の特定法則に従って移動機認証確認信号、加入者認証確認信号及び通信秘匿鍵を作成し、

前記移動機認証応答信号と該移動機認証確認信号、及び前記加入者認証応答信号と該加入者認証確認信号が一致するか否かを比較して前記通信相手を認証すると共に、該通信秘匿鍵の前記乱数による配送を行うことを特徴とするディジタル移動通信における認証方法。

【請求項２】　前記移動局における前記第２の秘密鍵の一部を、前記加入者の暗唱番号で置換えることを特徴とする請求項１記載のディジタル移動通信における認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ディジタル移動通信における基地局が、通信の相手の移動局が正当な移動局であることを認証するディジタル移動通信における認証方法に関する。

【０００２】

【従来の技術】近年、移動通信需要の増加、サービスの多様化の要求が高まるにつれて無線区間におけるセキュリティの保護が強く望まれている。一般に移動通信では、移動局と基地局とが通信毎に接続が変化するために、通信する移動局の正当性を加入者の収容位置で判定することができない。そのため、移動局の正当性をチェックするための認証機能が必要であると共に、パーソナル通信番号（ＰＴＮ）サービスでは通信を行う加入者の認証機能が必要である。また、無線回線を通信を用いることから通信内容を傍受される可能性があり、通信内容の機密保持のために通信内容を暗号化する秘匿機能が必要である。

【０００３】ここで、図４（Ａ），（Ｂ）に、従来の認証方法を説明するための図を示す。図４（Ａ），（Ｂ）

2

は、汎ヨーロッパ自動車電話方式における認証及び通信秘匿鍵の配送方法を示したものである。図４（Ａ）において、まず、固定網側は、乱数ＲＡＮＤ（認証要求信号）を移動局へ送信する。移動局は暗号化回路５１ａにおいて、ＤＥＳ（Data Encryption Standard）等のアルゴリズムＡ３に従い、予め移動局内に保持されている認証の鍵Ks と乱数ＲＡＮＤとからＳＲＥＳ（認証応答信号）を算出し、固定網側へ送信する。

【０００４】一方、固定網側では乱数ＲＡＮＤと、固定網側に予め保持されている認証の鍵K_S とを暗号化回路５１ｂ（暗号化回路５１ａと同じ）においてアルゴリズムＡ３に従いＳＲＥＳを算出する。そして、比較回路５２において、固定網側で算出したＳＲＥＳと移動局から送信されたＳＲＥＳとを比較し、一致（ｙｅｓ）であれば通信が開始され、不一致（ｎｏ）であれば通信不能となる。すなわち、固定網側で受信したＳＲＥＳの正当性を確認して、移動局の認証を行うものである。

【０００５】また、図４（Ｂ）は通信秘匿鍵の配送方法を示すもので、通信秘匿鍵の配送は、図４（Ａ）の認証と同時に行われる。図４（Ｂ）において、固定網側は乱数ＲＡＮＤと認証の鍵K_S とにより暗号化回路５５ｂのアルゴリズムＡ８に従って通信秘匿鍵Ｋｅを算出して記憶部５６にストアする。一方、固定網側の通信秘匿鍵Ｋｅをそのまま移動局へ送信することはせず、乱数ＲＡＮＤ信号を用いて間接的に送信する。すわなち、移動局では乱数ＲＡＮＤと認証の鍵Ks とを暗号化回路５５ａのアルゴリズムＡ８に従って通信秘匿鍵Ke を算出し、記憶部５７にストアするものである。

【０００６】このように、暗号化回路５１ａ，５１ｂ及び５５ａ，５５ｂのアルゴリズムＡ３及びA8 を暗号化アルゴリズムにすることにより、第三者の盗聴及び不当な移動局の使用を防ぐことが可能であり、かつ、認証以後の通信を秘匿するための秘匿鍵を暗号化して配送することを認証と同時に実現できる。

【０００７】

【発明が解決しようとする課題】しかし、上述の方法では認証の鍵Ks による１種類の認証しか行わないため、移動局側の移動機と加入者を区別できず、例えば１台の移動機を複数の加入者で共用することができない。ただ、同じ手順を２回繰り返すことにより、加入者認証と移動機認証を別々に行うことは可能であるが、無線伝送する信号量が２倍になり、スループットが低下するため、収容できる加入者数が減ってしまうという問題があった。また、認証の鍵K_S は、移動機内に保持されているため、移動機本体が盗まれた場合、不当な使用が可能になるという問題があった。

【０００８】そこで、本発明は上記課題に鑑みなされたもので、無線のスループットの低下を防止して１台の移動局を複数の加入者で共用することができると共に、盗難による不当な使用を防止するディジタル移動通信にお

ける認証方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】上記課題は、移動局側の移動機と基地局との間で移動通信を行うにあたり、通信相手の認証を行い、通信を開始するか否かの判断を行うためのディジタル移動通信における認証方法において、前記移動局は、前記基地局より送られた所定の乱数と、予め保持されている移動機固有の第１の秘密鍵とにより第１の特定法則に従って移動機認証応答信号を作成して該基地局に送信し、該乱数と加入者からの加入者固有の第２の秘密鍵とにより第２の特定法則に従って加入者認証応答信号を作成して該基地局に送信し、該乱数と該第１及び第２の秘密鍵とにより第３の特定法則に従って通信を秘匿する通信秘匿鍵を作成し、前記基地局は、該基地局で発生させた該所定の乱数と、予め保持されている前記第１及び第２の秘密鍵とにより、前記第１，第２及び第３の特定法則に従って移動機認証確認信号、加入者認証確認信号及び通信秘匿鍵を作成し、前記移動機認証応答信号と該移動機認証確認信号、及び前記加入者認証応答信号と該加入者認証確認信号が一致するか否かを比較して前記通信相手を認証すると共に、該通信秘匿鍵の前記乱数による配送を行うことにより、または前記移動局における前記第２の秘密鍵の一部を、前記加入者の暗唱番号で置換えることにより解決される。

【００１０】

【作用】上述のように、基地局より所定の乱数を移動局に送り、移動局でこの乱数と第１及び第２の秘密鍵とにより移動機認証応答信号及び加入者認証応答信号を作成する。一方、基地局では該乱数と予め保持されている第１及び第２の秘密鍵とにより移動機認証確認信号及び加入者認証確認信号を作成する。そして、基地局で当該応答信号と確認信号とを比較して、一致した場合に通信を開始するものである。

【００１１】すなわち、一度の認証手順で移動機認証と加入者認証を同時に行うことにより、無線のスループットを低下させることなく１台の移動機を複数の加入者で共用することが可能となる。また、第２の秘密鍵の一部を加入者の暗唱番号に置換えることにより、移動機本体が盗まれた場合に不当な使用を防止することが可能となる。

【００１２】また、移動局及び基地局は、乱数と第１及び第２の秘密鍵により通信秘匿鍵を作成する。すなわち、上述の応答信号及び確認信号が一致した場合には、移動局及び基地局両方における通信秘匿鍵が正しく共有されたこととなる。従って、移動機認証、加入者認証及び通信秘匿鍵の配送を同時に行うことが可能となる。

【００１３】

【実施例】図１に、本発明の一実施例のブロック図を示す。図１中、３０は移動局における移動機、３１は基地局の乱数発生回路、３２は基地局の信号変換回路、３３は移動局の信号変換回路、３４は基地局の比較回路をそれぞれ表している。信号変換回路３２と３３は同じ機能秘密，鍵Kp を共有する。加入者の秘密鍵K_p は、例えば、ＩＣカード等に記録され、使用時に移動機３０に挿入する等、移動機３０と加入者が分離した形態である。

【００１４】基地局は、まず乱数発生回路３１で、認証要求用の乱数Ｒを発生し、移動局へ送信する。暗号強度の観点から、乱数Ｒのビット長は６４ビット程度以上が望ましい。

【００１５】移動機３０は、受信した乱数Ｒと、移動機の秘密鍵Ks と、加入者カードから読み出した加入者の秘密鍵Kp を信号変換回路３３に入力し、認証応答Rs1，Rp1及び通信秘匿鍵Ke1を得る。この通信秘匿鍵Ke2は以後の通信を秘匿するための通信秘匿鍵として用いる。そして、認証応答Rs1，Rp1は基地局へ送信される。

【００１６】基地局は、乱数発生回路３１で発生した乱数Ｒと秘密鍵Ks 及びKp を信号変換回路３２に入力し、認証応答Rs2，Rp2及び通信秘匿鍵Ke2を得る。通信秘匿鍵Ke2は以後の通信を秘匿するための通信秘匿鍵として用いる。比較回路３４は、移動局から受信した認証応答Rs1，Rp1、及び基地局内で発生した信号Rs2，Rp2を入力し、それぞれのビットパターン（ビット列の配列）を比較する。Rs1とRs2が等しいとき移動機認証ＯＫとし、それ以外のとき移動機認証ＮＧとする。又Rp1とRp2が等しいとき加入者認証ＯＫとし、それ以外のとき加入者認証ＮＧとする。それぞれのビットパターンが一致するということは、移動局と基地局の秘密鍵Ks 及びKp が同じである（従って通信の相手の移動局が正当な移動局である）ことを意味し、認証要求と認証応答が誤り無く伝送された（従って通信秘匿鍵が正しく共有された）ことを高い確率で保証する（信頼度はＲとRs1及びRp1のビット数を多くする程高くなる）。

【００１７】なお、移動局の加入者の秘密鍵Kp は、一部を移動機３０内の不揮発性メモリに記録し、残りは加入者が暗証番号として記憶し、通信を開始するとき等にテンキー等により移動機３０に入力してもよい。また、暗証番号とメモリ上の番号との、ある特定の演算で得られる結果を秘密鍵とする場合であってもよい。これによれば、移動機３０が盗まれても暗証番号がわからなければ、不当な使用が不可能になる。

【００１８】次に、図２に、図１の移動機における信号変換回路の一具体例のブロック図を示す。図２の信号変換回路３３中、４１は第１の暗号化回路、４２は第２の暗号化回路，４３は第３の暗号回路，４４は多重化回路をそれぞれ表わしている。なお、基地局の信号変換回路３３においても多重化回路４４を除き同じ構成である。また、第１～第３の暗号化回路は同一の回路構成でもよい。

【００１９】第１の暗号化回路４１は、加入者の秘密鍵

Kp を用いて、基地局から受信した認証要求用の乱数Rを第２の特定法則に従い３２ビットで暗号化し、認証応答Rplを出力する。第２の暗号回路４２は、移動機３０の秘密鍵Ks を用いて乱数Rを第１の特定法則に従い、３２ビットで暗号化し、認証応答Rslを出力する。第３の暗号化回路４３は、移動機３０の秘密鍵Ks を用いて、認証応答Rslを第３の特定法則に従い、暗号化し、通信秘匿鍵Kelを出力する。また、多重化回路４４は、RslとRplを多重化し、一信号として基地局に出力する。なお、多重化回路４４を外し、RslとRplを別信号として送信してもよい。

【００２０】第１～第３の暗号化回路４１，４２及び４３で実現する暗号は、移動機３０内実現するため、回路規模が小さく処理量が少ないことが必要である。このような第１～第３の特定法則による暗号化方式としては例えばＦＥＡＬ（Fast data Encipherment Algorithm），ＤＥＳ等の秘密鍵暗号方式が有効である。従って、上記の暗号秘匿鍵Kelを導出することが現実に極めて困難なため、認証以降の通信を盗聴すること、及び不当な移動局を作成して使用することが、現実的には不可能である。なお、出力信号Rsl，Rplのビット数は入力信号Rとは同じにするのが信頼度の点で良いが、入力信号Rのビット数が充分大きければ、出力信号Rsl，Rplのビット数を入力信号より少なくし、無線のスループットを向上させてもよい。例えば、暗号方式としてＦＥＡＬを採用する場合、図１のように、入力信号Ｒを６４ビットとすると出力信号Rsl，Rplは共に６４ビットとなるが、それぞれの下位３２ビットのみを抽出し、多重化して６４ビットの認証応答を構成して送信する。これによれば、盗聴して秘密鍵を算出することが一層困難になる。なお、上記実施例は、単に基地局と表現したが、基地局の上位の制御局，交換局，ホームメモリ局等を含む。

【００２１】次に、図３に、本発明の他の実施例のブロック図を示す。図３（Ａ）はユーザ間で認証を行う場合の概要を示したもので、図３（Ｂ）は、図３（Ａ）を図１に対応させて説明するためのブロック図である。図３（Ａ）において、認証起動ユーザ（図１における基地局に相当）と被認証側ユーザ（図１における移動局に相当）間で認証を行うもので、秘密の暗号鍵K_i（図１におけるKp，Ks に相当）を共有する。

【００２２】いま、認証起動側ユーザは適当な平文Ｐ（図１における乱数Rに相当）を被認証側ユーザに送信すると共に、平文Ｐと暗号鍵Ki を用いて暗号Ｃ（図１におけるRs2，Rp2に相当）を生成する。一方、被認証側ユーザでは、受信した平文Ｐから暗号鍵Ki を用いて暗号文Ｃ’（図１におけるRsl，Rplに相当）を生成し、認証起動側ユーザに返送する。暗号文ＣとＣ’が等しければ認証ＯＫである。

【００２３】このように、平文Ｐを認証毎に異なった文（乱数）にすることにより、認証手順の内容を呼毎に変えることができ、秘匿性が高い認証方法を実現することができる。

【００２４】また、図３（Ｂ）において、移動交換機（認証起動ユーザ）の暗号化器Ｆ’（図１における信号変換回路３２に相当）及び移動機（被認証ユーザ）の暗号化器Ｆ，Ｆ”（図１における信号変換回路３３に相当）では、暗号化速度を速くし、移動機のＣＰＵ（中央処理装置）に対する負担を小さくするために、前述のＦＥＡＬ、ＤＥＳ等の秘密鍵暗号を用いる。なお、認証鍵Ki である加入者用認証鍵Kp 及び移動機用認証鍵Ksは加入者データの一部としてホームメモリ局に格納する。

【００２５】まず、移動交換機は移動機に対して、移動交換機内で発生した乱数Ｒ（Ｐ）を送信して認証要求を行う。そこで、移動機では、受信したＲ（Ｐ）を加入者用と移動機用の認証鍵であるKp，Ks （Ki ）を用いて暗号化器Ｆ及びＦ”にて暗号化結果Rp，Rs （図３（Ａ）におけるＣ’，図１におけるRpl，Rsl2 相当）を得る。移動交換機においても同様にホームメモリより認証鍵Kp，Ks （Ki ）を取出して処理を行う。

【００２６】そして、移動機は移動交換機に該暗号化結果Pp，Rs を認証応答として送信する。移動交換機では両者の暗号化結果を比較照合し、結果が一致した場合に認証正常とみなして、通信を開始するものである。なお、図２では移動秘密鍵Ksより秘匿鍵Kelを生成しており、図３（Ｂ）では加入者用認証鍵K_p より秘匿鍵Kelを生成しているが、両者は必ずしも別のものではなく、移動交換機側と統一されていればどちらでもよい。

【００２７】ここで、認証手順中に生成される暗号化結果を秘匿鍵に利用すれば（移動機の秘匿鍵Kel及び移動交換機の秘匿鍵Ke2）、無線回線における秘匿鍵の配送を安全かつ効率的に実現でき、また呼毎に異なった秘匿鍵を生成できることから秘匿パターンを呼毎に変えられ、安全性の高い秘匿ができる。

【００２８】

【発明の効果】以上のように本発明によれば、１回の認証手順で、移動機認証と加入者認証を同時に実現することにより、無線のスループットを下げることなく、１台の移動機を複数の加入者で共用することができ、秘密鍵の一部を暗証番号とすることにより、移動本体が盗まれても暗証番号により不当な使用を防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施例のブロック図である。

【図２】図１の移動機における信号交換換回路の一具体例のブロック図である。

【図３】本発明の他の実施例のブロック図である。

【図４】従来の認証方法を説明するための図である。

【符号の説明】

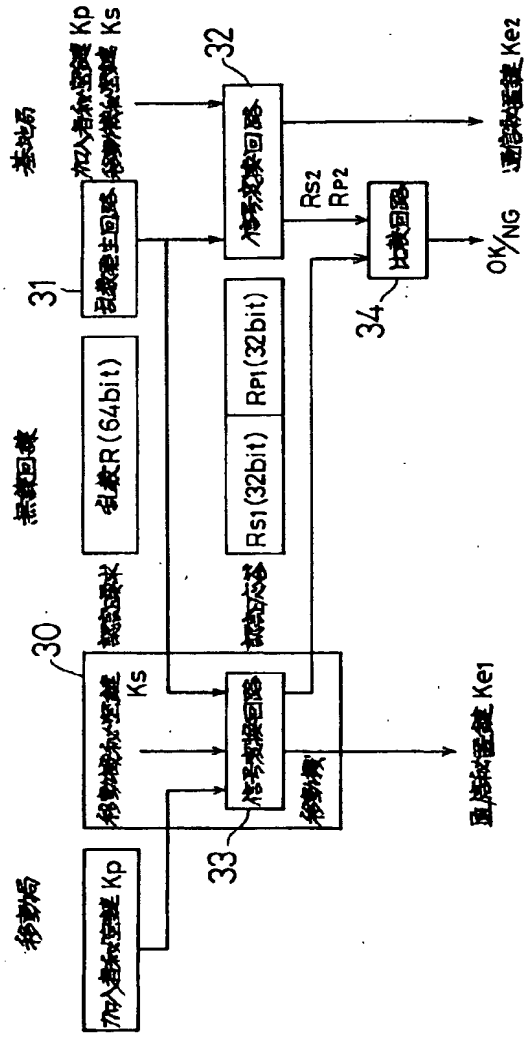
３０　移動機

7　　8

３１　乱数発生回路
３２，３３　信号変換回路
３４　比較回路
４１　第１の暗号化回路
４２　第２の暗号化回路
４３　第３の暗号化回路
４４　多重化回路

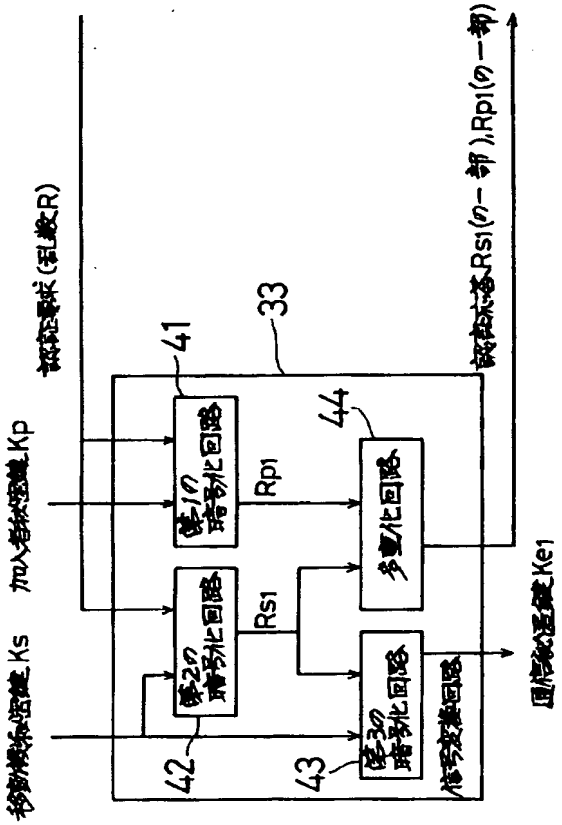
【図１】

本発明の一実施例のブロック図



【図2】

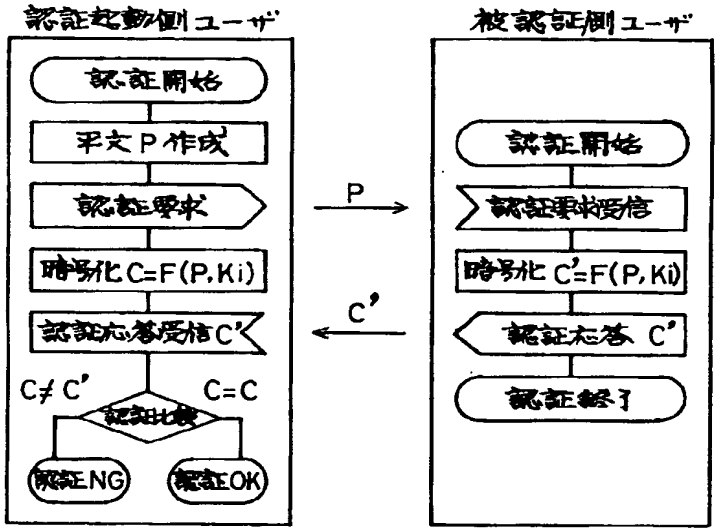
図1の移動機における信号変換回路の一具体例のブロック図



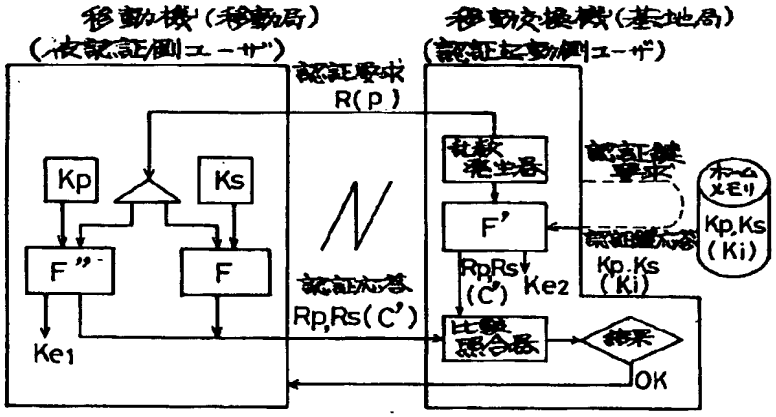
【図3】

本発明の他の実施例のブロック図

(A)

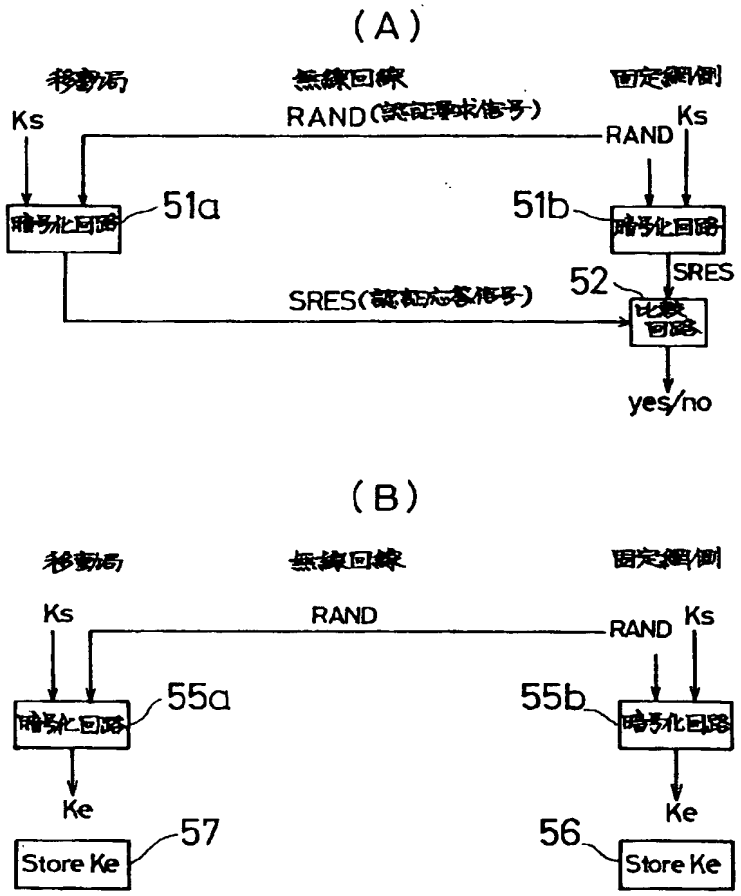


(B)



【図４】

従来の認証方法を説明するための図



フロントページの続き

(72)発明者　尾上　誠蔵
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　花岡　光昭
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内

(72)発明者　中村　寛
東京都千代田区内幸町一丁目１番６号　日本電信電話株式会社内